**REGULAMENTO DE**

**SISTEMA**

(«*Nome da ORGANIZAÇÃO*»)

Versão: 1.0

Este regulamento não pode ser reproduzido nem a sua estrutura reutilizada a não ser com a autorização expressa e por escrito do seu autor i.e. TIC – Tecnologia Informática e Computadores Lda.

1. INTRODUÇÃO

Este regulamento tem como objetivo estabelecer as diretrizes de utilização do SISTEMA. Pretende contribuir para a implementação de uma cultura atenta às questões de segurança, privacidade, integridade e disponibilidade dos dados dentro da ORGANIZAÇÃO, estabelecendo regras conducentes à conformidade com a legislação em vigor, nomeadamente com o Regulamento Geral de Proteção de Dados (RGPD).

Os objetivos principais deste documento são: i) definir as regras de utilização do SISTEMA; ii) consciencializar os utilizadores do papel que desempenham na segurança e privacidade do SISTEMA; iii) atribuir responsabilidades de registos de verificação de bom funcionamento de componentes (e.g. estabilizador de energia) e cópias de segurança; iv) definir boas práticas de utilização; e v) definir a forma de verificar e reavaliar periodicamente o cumprimento do regulamento.

* 1. Definições e acrónimos

Neste documento são utilizados a seguinte terminologia e acrónimos:

* + 1. «ORGANIZAÇÃO» - a empresa ou conjunto de empresas (i.e. grupo de empresas) que partilham o mesmo SISTEMA total ou parcialmente.
    2. «SISTEMA» - refere o conjunto de dispositivos, infraestruturas, utilizadores e parceiros, que constituem o sistema informático da ORGANIZAÇÃO. Consideram-se pertencentes ao SISTEMA os dispositivos ligados de forma permanente (e.g. impressora ligada por rede) ou não (e.g. disco externo ou *pendrive* ligada conectada por USB).
    3. «RGPD» - é a sigla pelo qual é conhecido o Regulamento Geral de Proteção de Dados EU 2016/679.
    4. «DADOS PESSOAIS» - informação relativa a uma pessoa singular identificada ou identificável direta ou indiretamente através de um ou conjugação de vários dados ou características (RGPD, Art.º 4, N.º 1).
    5. «DADOS PESSOAIS SENSÍVEIS» - são DADOS PESSOAIS cuja violação pode implicar um elevado risco para os direitos e liberdades das pessoas singulares (RGPD, Art.º 34, N.º 1).
    6. «TITULAR DOS DADOS» ou «TITULARES DOS DADOS» - o TITULAR DOS DADOS é o dono dos DADOS PESSOAIS ou DADOS PESSOAIS SENSÍVEIS.
    7. «DPO» - é o acrónimo para *Data Protection Officer* (Encarregado de proteção de dados).
  1. Intervenientes

No decurso deste documento são mencionados vários intervenientes que agora se apresentam:

* + 1. «RESPONSÁVEL PELO TRATAMENTO» - pessoa singular ou coletiva que individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de DADOS PESSOAIS (RGPD, Art.º 4, N.º 7). É o responsável final pelo cumprimento das obrigações da ORGANIZAÇÃO (e.g. gerente ou administrador).
    2. «UTILIZADOR» OU «UTILIZADORES» - pessoa autorizada pelo RESPONSÁVEL PELO TRATAMENTO a manusear parcial ou totalmente, e física ou remotamente o SISTEMA.
    3. «AUDITOR» - pessoa designada pelo RESPONSÁVEL PELO TRATAMENTO para efetuar auditorias periódicas com o objetivo de garantir o cumprimento deste regulamento, levantar vulnerabilidades e propor medidas corretivas para as resolver ou mitigar.
    4. «ADMINISTRADOR DE SISTEMA» - pessoa designada pelo RESPONSÁVEL PELO TRATAMENTO para a manutenção técnica da infraestrutura do SISTEMA, de sua confiança, com o objetivo de promover o seu bom funcionamento.
  1. Objeto e âmbito

Com este regulamento o RESPONSÁVEL PELO TRATAMENTO demonstra a preocupação da ORGANIZAÇÃO com a segurança, privacidade e integridade dos dados, e com a disponibilidade do SISTEMA. Neste contexto, expressa a vontade de implementar regras e boas práticas conducentes à conformidade com o RGPD e demais legislação.

Este documento regulamenta apenas os aspetos de privacidade, segurança, integridade e disponibilidade relacionados com o SISTEMA. São âmbito todos os dispositivos ligados ou integrados através de qualquer tipo de conexão (e.g. rede, USB). Não são considerados âmbito deste regulamento: i) os dispositivos sem ligação ou integração direta com o SISTEMA (e.g. relógio de ponto de cartões em papel, videovigilância por cabo coaxial, etc.); ii) informação constante em papel (e.g. capas de arquivo); etc.

* 1. Organização e documentação

O RESPONSÁVEL PELO TRATAMENTO acredita que um SISTEMA devidamente documentado e organizado é mais fácil de evoluir e manter. Além disso uma boa organização facilita os processos de auditoria de revisão e fiscalização a que está sujeito (e.g. Autoridade de Controlo e outras entidades).

* + 1. O RESPONSÁVEL PELO TRATAMENTO designa o AUDITOR para a elaboração e manutenção do *dossier* do SISTEMA, cuja leitura deve:
       1. Facilitar a identificação dos componentes de SISTEMA;
       2. Apresentar o Plano de Segurança e Disponibilidade em vigor;
       3. Registar as vulnerabilidades e medidas corretivas identificadas e corrigidas ao longo do tempo.
    2. A estrutura do *dossier* deve conseguir agregar de forma organizada toda informação relacionada com os componentes do SISTEMA, detalhes do Plano de Segurança e Disponibilidade, documentação das auditorias, e todos os registos produzidos pelos UTILIZADORES e AUDITOR. Pretende-se demonstrar a evolução do SISTEMA, focada nos objetivos de melhoria contínua e iterativa dos fatores de segurança e privacidade ambicionados pela ORGANIZAÇÃO.
    3. O *dossier* deve ser mantido em total sigilo, podendo apenas ser editado pelo AUDITOR, e consultado pelo RESPONSÁVEL PELO TRATAMENTO e pelo ADMINISTRADOR DE SISTEMA.
    4. Aproveitando o facto de se reunir toda a informação relativa ao SISTEMA, o *dossier* deve contemplar na sua organização o arquivo dos comprovativos de compra e licenciamento com o objetivo de facilitar os processos inspetivos de outras autoridades de fiscalização (e.g. fiscalização de licenciamento).
  1. Obrigações do RESPONSÁVEL PELO TRATAMENTO

Este documento regulamenta um conjunto de normas e boas práticas de utilização que visa a privacidade, segurança, disponibilidade e integridade dos dados do SISTEMA. Constituem responsabilidades do RESPONSÁVEL PELO TRATAMENTO:

* + 1. Avaliar e decidir acerca da necessidade de um DPO no SISTEMA.
    2. Designar o AUDITOR e ADMINISTRADOR DE SISTEMA.
    3. Promover o cumprimento deste regulamento.
  1. Obrigações dos UTILIZADORES

Os UTILIZADORES devem cumprir e promover o cumprimento das regras definidos neste regulamento, e pelos outros instrumentos ou documentos originários deste (i.e. registos, normas, procedimentos, etc.).

Além disso, os UTILIZADORES são:

* + - 1. Responsáveis por seguir uma política de total sigilo relativamente ao SISTEMA não partilhando qualquer informação com estranhos (e.g. configurações de dispositivos, existência de ligações remotas, dispositivos amovíveis que são transportados para fora da ORGANIZAÇÃO, etc.).
      2. Responsáveis por manter em total sigilo e nunca partilhar com ninguém as palavras-chave de acesso ao SISTEMA.
      3. Responsáveis pela utilização cuidada de todos os componentes (e.g. dispositivo), com o objetivo de promover o bom funcionamento do SISTEMA.
      4. Responsáveis por executar com zelo as responsabilidades de registo atribuídas pelo RESPONSÁVEL PELO TRATAMENTO.
      5. Responsáveis por alertar o RESPONSÁVEL PELO TRATAMENTO e ADMINISTRADOR DE SISTEMA de qualquer mau funcionamento de componente, mesmo que seja apenas um receio com necessidade de confirmação técnica.
      6. Responsáveis por alertar o RESPONSÁVEL PELO TRATAMENTO e ADMINISTRADOR DE SISTEMA para qualquer evento ou configuração que pareça desrespeitar ou ferir este regulamento, ou que se suspeite que possa por em risco de qualquer forma o SISTEMA ou a informação que armazena.

1. PRIVACIDADE E SEGURANÇA

O RESPONSÁVEL PELO TRATAMENTO em conjunto com os UTILIZADORES assumem o compromisso de tudo fazer para que o SISTEMA mantenha bons níveis de segurança e disponibilidade. O objetivo principal deste compromisso é proteger os dados dificultando ao máximo a possibilidade de acesso não autorizado por estranhos ao SISTEMA.

Neste sentido, o RESPONSÁVEL PELO TRATAMENTO compromete-se a dotar o SISTEMA com os mecanismos de segurança recomendados pelo AUDITOR e ADMINISTRADOR DO SISTEMA, pesando sempre com bom senso o esforço de investimento de cada medida proposta e o impacto que pode representar na privacidade, segurança, integridade e disponibilidade nos dados e no SISTEMA.

Os UTILIZADORES comprometem-se a utilizar o SISTEMA tendo por base critérios de utilização responsável e a olhar para a privacidade dos dados como algo essencial para o sucesso da ORGANIZAÇÃO.

O RESPONSÁVEL PELO TRATAMENTO acredita que a demonstração de conformidade com a legislação em vigor relativa à proteção de dados (e.g. RGPD) aumentará a confiança do mercado na ORGANIZAÇÃO, conduzirá à conquista de novos clientes e manutenção dos atuais.

* 1. Infraestrutura

A configuração da infraestrutura deve impedir por defeito todos os acessos à infraestrutura (i.e. por defeito, a infraestrutura deve recusar todas as ligações e dispositivos). Esta medida pretende proibir por defeito: i) todos os acessos a partir da internet a não ser os expressamente autorizados pelo RESPONSÁVEL PELO TRATAMENTO; e ii) a ligação descontrolada de novos dispositivos à rede local sem uma prévia avaliação de impacto no SISTEMA e uma configuração apropriada (e.g. computadores com *malware*).

* + 1. A infraestrutura deverá estar dotada de mecanismos que:
       1. Permitam que as barreiras de acesso estejam sobre o total domínio de configuração da ORGANIZAÇÃO (e.g. o router da rede interna apenas pode ser configurado pelo ADMINISTRADOR DO SISTEMA e acedido pelo AUDITOR para fins de auditoria);
       2. Impeçam o acesso à infraestrutura por estranhos ao SISTEMA a partir da internet, mas que permitam configurar exceções que possam vir a ser autorizadas pelo RESPONSÁVEL PELO TRATAMENTO.
    2. Deverão ser implementados mecanismos de barreira que permitam controlar a admissão de novos dispositivos à rede local, evitando:
       1. Tentativas de ligação de dispositivos não previstos pelo ADMINISTRADOR DO SISTEMA;
       2. Configurações erradas que possam por em causa a integridade dos dados e do SISTEMA.
    3. Não são admitidos distribuidores de rede sem fios dentro do SISTEMA. No entanto, é admissível que existam na parte pública da rede (i.e. fora do SISTEMA).
    4. Apesar dos riscos inerentes à utilização de distribuidores de rede sem fios, a ORGANIZAÇÃO assume a necessidade de os correr porque existem dispositivos com necessidades de comunicar sem fios no SISTEMA. Ciente dos riscos, o RESPONSÁVEL PELO TRATAMENTO autoriza e justifica em ata arquivada no *dossier* de sistema a necessidade de recorrer a este tipo de comunicação dentro da ORGANIZAÇÃO. No entanto, e com o objetivo de mitigar as vulnerabilidades associadas à comunicação sem fios:
       1. Os distribuidores devem disponibilizar de mecanismos de admissão de novos dispositivos sem fios;
       2. Devem ser implementados mecanismos que impeçam que os dados transmitidos no meio sem fios não possam facilmente ser lidos ou interpretados por estranhos ao SISTEMA;
       3. A chave de acesso deve ser composta por: i) 5 letras maiúsculas; ii) 5 minúsculas; iii) 5 números; e iv) 5 caracteres não alfanuméricos. A ordem da disposição das letras, números e caracteres, deve ser totalmente aleatória e não podem constituir palavras;
       4. A chave de acesso deve ser alterada a cada 12 meses e sempre que existe a saída de um UTILIZADOR que tenha trabalhado com um dispositivo com comunicação sem fios, ou que possa ter acesso de alguma forma à chave de segurança;
       5. A chave deve apenas ser de conhecimento do RESPONSÁVEL PELO TRATAMENTO e do ADMINISTRADOR DO SISTEMA. Nunca deve ser divulgada mesmo aquando da configuração de um dispositivo sem fios;
       6. A atualidade da necessidade de existir distribuidores de rede sem fios dentro do SISTEMA deve ser reavaliada a cada 12 meses.
    5. O AUDITOR deve verificar a cada auditoria que as atualizações de segurança dos dispositivos (e.g. *firmware*) esteja na última versão estável disponibilizada pelos fabricantes.
    6. Todas as regras de exceção de acesso à infraestrutura devem ser revistas a cada 12 meses com o objetivo de avaliar a sua pertinência e atualidade.
  1. Computadores

A configuração dos computadores deve, por defeito, impedir todos os acessos ao sistema operativo (i.e. o sistema operativo deve recusar por defeito todas as ligações que lhe sejam solicitadas). Esta medida funciona como: i) uma barreira de segunda linha às solicitações de acesso com origem na internet; e ii) como barreira numa tentativa de acesso não autorizado a partir da rede local (e.g. *malware* noutro computador, ataque a partir de um dispositivo com *firmware* comprometida, etc.).

* + 1. Os computadores devem conter aplicações devidamente configuradas, ativas, atualizadas e em funcionamento que:
       1. Impeçam o acesso por estranhos ao computador a partir da internet e da rede local, mas que permitam configurar exceções para utilização de recursos partilhados na rede ou acessos externos que estejam ou possam vir a estar autorizados pelo RESPONSÁVEL PELO TRATAMENTO;
       2. Protejam e previnam a propagação de *malware* no computador e no SISTEMA;
       3. No caso de serem movidos com dados guardados localmente (e.g. computadores portáteis, computadores fixos para reparação externa, etc.), esses dados sejam ilegíveis (e.g. encriptação) a estranhos ao SISTEMA (e.g. furto ou extravio);
       4. A configuração dessas aplicações apenas poderá estar disponível ao ADMINISTRADOR DO SISTEMA;
       5. Todas as regras de exceção de acesso ao SO dos computadores devem ser revistas a cada 12 meses com o objetivo de avaliar a sua pertinência e atualidade.
    2. O ADMINISTRADOR DE SISTEMA deve configurar os dispositivos para que os UTILIZADORES não possam alterar as configurações do sistema operativo e restantes aplicações, e instalar ou desinstalar irregularmente programas. Além disso, o ADMINISTRADOR DE SISTEMA deve garantir que:
       1. Os UTILIZADORES não trabalhem nos computadores com direitos de administrador;
       2. Todas as contas configuradas nos computadores (i.e. administradores e utilizadores) estão configuradas com palavras-chave e não existem contas de acesso livre (i.e. sem palavra-chave) (e.g. conta de convidado);
       3. As contas configuradas nos computadores não identifiquem os UTILIZADORES que utilizam cada dispositivo;
       4. Os nomes dos diversos dispositivos não identifiquem os UTILIZADORES que os utilizam;
       5. Os computadores apenas disponibilizam os recursos autorizados, com as permissões definidas para cada recurso pelo RESPONSÁVEL PELO TRATAMENTO;
       6. Os computadores bloqueiam automaticamente a sessão de trabalho após 5 minutos de inatividade e, para retomar a sessão, o UTILIZADOR tem que inserir a sua palavra-passe;
       7. As aplicações instaladas se mantenham atualizadas para promover o aumento do nível de segurança, diminuindo a hipótese de ataque ou acesso por estranhos ao computador e ao SISTEMA;
       8. Apenas existam configuradas regras de exceção nas *firewall* de SO estritamente necessárias ao funcionamento autorizado do SISTEMA pelo RESPONSÁVEL PELO TRATAMENTO;
    3. São obrigações do UTILIZADOR:
       1. Manter reserva dos dados quando outro UTILIZADOR ou pessoa estranha ao SISTEMA está próximo do seu monitor;
       2. Bloquear a sessão de trabalho do computador sempre que se ausenta da frente do monitor, mesmo estando ativo o bloqueio automático de sessão.
       3. Proceder à comunicação imediata ao RESPONSÁVEL PELO TRATAMENTO, aquando a verificação furto ou extravio de um computador passível de ser movido com dados guardados localmente.
    4. O AUDITOR deve verificar a cada auditoria que as atualizações de segurança de SO e aplicações estejam na última versão estável disponibilizada pelos fabricantes.
  1. Recursos de rede

Os recursos de rede, enquanto repositórios de dados no SISTEMA, devem obedecer a critérios rígidos e bem definidos em termos de estrutura e permissões de acesso. Os dados constantes no SISTEMA estão intrinsecamente ligados a cada organização. Por esse motivo, a estratégia de arquivo é delineada pelo RESPONSÁVEL PELO TRATAMENTO porque é o conhecedor holístico de toda a atividade operacional da ORGANIZAÇÃO.

* + 1. Assim, o RESPONSÁVEL PELO TRATAMENTO deve:
       1. Definir a estrutura de recursos de rede (i.e. partilhas) e respetivas pastas e subpastas, seguindo uma estratégia que facilite a gestão de acessos (i.e. permissões) com base em palavras-chave. Esta estrutura deve facilitar a localização de dados com o objetivo de: i) promover a produtividade dos UTILIZADORES no exercício das suas funções no SISTEMA; e ii) incentivar que os UTILIZADORES guardem a informação respeitando a estratégia inicialmente desenhada;
       2. Definir quem tem acesso a cada recurso e com que direitos (i.e. leitura e escrita ou somente leitura).
    2. O ADMINISTRADOR DE SISTEMA deve configurar:
       1. Os recursos de rede mediante a estrutura dada pelo RESPONSÁVEL PELO TRATAMENTO;
       2. Os acessos a cada recurso com palavras-chave para garantir que apenas os UTILIZADORES autorizados acedem a cada recurso.
    3. A localização rápida da informação é importante para a produtividade dos UTILIZADORES, mas também para facilitar o cumprimento de obrigações pela ORGANIZAÇÃO. Com o objetivo de promover o princípio da minimização de informação considera-se como obsoletos todos os dados:
       1. Desnecessários ao exercício operacional da ORGANIZAÇÃO sem necessidade legal de mantenimento;
       2. Não acedidos há mais de 24 meses cujo prazo de manutenção não está regulamentado por legislação;
       3. Não acedidos há mais tempo do que o prazo regulamentado pela legislação em vigor.
    4. Os UTILIZADORES devem:
       1. Respeitar a estrutura de partilhas, pastas e subpastas definida pelo RESPONSÁVEL PELO TRATAMENTO, participando da estratégia de organização da informação no SISTEMA;
       2. Promover que apenas exista no SISTEMA informação necessária ao exercício da atividade operacional da ORGANIZAÇÃO, seguindo o princípio da minimização de ficheiros.
    5. É responsabilidade do AUDITOR verificar que:
       1. Apenas existam os recursos autorizados pelo RESPONSÁVEL PELO TRATAMENTO;
       2. As permissões de cada recurso sejam as definidas pelo RESPONSÁVEL PELO TRATAMENTO.
    6. A cada 12 meses o RESPONSÁVEL PELO TRATAMENTO deve:
       1. Verificar a atualidade e pertinência de cada recurso de rede;
       2. Validar que os ficheiros gerados pelos UTILIZADORES estão a ser corretamente arquivados respeitando a estrutura de partilhas e pastas que havia definido;
       3. Promover o apagamento da informação obsoleta;
       4. Garantir que apenas existem no SISTEMA os dados estritamente necessários à atividade operacional da ORGANIZAÇÃO: i) para promover que a informação é facilmente encontrada; e ii) garantir o cumprimento atempado das obrigações atribuídas legalmente ao RESPONSÁVEL PELO TRATAMENTO nomeadamente as relacionadas com a resposta ao exercício dos direitos pelos TITULARES DOS DADOS.
  1. Recursos externos

Os recursos externos permitem guardar informação em sistemas externos à ORGANIZAÇÃO (e.g. dropbox, googledrive, onedrive, etc.). Como são externos à empresa, devem obedecer a critérios ainda mais rígidos do que os definidos nos recursos de rede internos. Assim, os recursos externos têm que ser expressamente autorizados e justificados pelo RESPONSÁVEL PELO TRATAMENTO, por escrito, e essa autorização deve constar do *dossier* de SISTEMA.

* + 1. Não são admitidos recursos externos no SISTEMA, sejam eles sincronizados a partir de aplicações instaladas ou com utilização a partir de navegadores de internet.
    2. Não são admitidos recursos externos no SISTEMA que funcionem como sincronizadores de pastas locais. O acesso a recursos externos a partir de navegadores de internet tem que ser autorizado pelo RESPONSÁVEL PELO TRATAMENTO:
       1. Os UTILIZADORES com acesso serão identificados no *dossier* de SISTEMA, e apenas estes podem conhecer as credenciais de acesso ao recurso externo;
       2. A autorização deve constar no *dossier* de SISTEMA assim como a justificação e conteúdo de cada recurso autorizado;
       3. Os dados apenas podem ser mantidos nesses recursos enquanto fizer sentido no contexto da autorização feita pelo RESPONSÁVEL PELO TRATAMENTO;
       4. A necessidade de cada recurso externo deve ser reavaliada a cada 6 meses.
    3. São admitidos recursos externos no SISTEMA que funcionem como sincronizadores de pastas locais. O acesso a recursos externos tem que ser autorizado pelo RESPONSÁVEL PELO TRATAMENTO no *dossier* de SISTEMA e deve:
       1. Identificar quais os UTILIZADORES com acesso e sem conhecimento das credenciais de acesso ao serviço;
       2. Identificar quais os UTILIZADORES com acesso e com conhecimento das credenciais de acesso ao serviço;
       3. Identificar que dados estão autorizados a serem guardados nesse recurso externo;
       4. Prever que os dados apenas podem ser mantidos nesses recursos enquanto fizer sentido no contexto da autorização feita pelo RESPONSÁVEL PELO TRATAMENTO;
       5. Ser reavaliada a necessidade de existirem recursos externos a cada 6 meses.
  1. Utilizadores e palavras-chave

Os UTILIZADORES devem utilizar os dispositivos de forma responsável e com bom senso. Devem estar atentos a qualquer comportamento estranho do SISTEMA, reportando-o imediatamente ao ADMINISTRADOR DO SISTEMA e RESPONSÁVEL PELO TRATAMENTO.

As palavras-chave são códigos que autenticam o acesso e têm grande impacto na segurança de todo o SISTEMA.

* + 1. Sempre que possível, todos os dispositivos devem estar protegidos com palavras-passe para vedarem o acesso não autorizado à informação ou configurações existentes (e.g. computadores, routers, impressoras, etc.).
    2. As palavras-chave de computadores e restantes dispositivos do SISTEMA devem:
       1. No caso de utilizadores com permissões de administração, ser constituídas no mínimo por 13 caracteres: 3 letras maiúsculas (e.g. H, F, Z, etc.); 3 letras minúsculas (e.g. y, a, p, etc.); 3 números (e.g. 6, 1, 4, etc.); e 4 caracteres não alfanuméricos (e.g. $, !, ;, etc.);
       2. No caso de utilizadores sem permissões de administração, ser constituídas no mínimo por 9 caracteres: 2 letras maiúsculas; 2 letras minúsculas; 2 números; e 3 caracteres não alfanuméricos;
       3. A ordem da disposição das letras, números e caracteres não alfanuméricos, deve ser totalmente aleatória e não pode constituir uma palavra (e.g. Ae!W/9#2t1;Jr);
       4. Devem ser criadas pelo ADMINISTRADOR DO SISTEMA para garantir o cumprimento das regras deste regulamento e a complexidade necessária na tentativa de prevenir que sejam descobertas por estranhos ao SISTEMA;
       5. Devem ser guardadas em envelope fechado, mantidas em local reservado apenas acessível ao RESPONSÁVEL PELO TRATAMENTO e ADMINISTRADOR DO SISTEMA;
       6. Devem ser modificadas: i) a cada 6 meses; ii) sempre que exista a saída de um UTILIZADOR do SISTEMA (neste caso apenas têm que ser alteradas as palavras-chave conhecidas ou que possam ser conhecidas do UTILIZADOR em causa); na admissão de um novo dispositivo com o objetivo de substituir a palavra-chave original; ou iii) quando existe a suspeita ou indício de acesso indevido por outros UTILIZADORES ou por pessoas estranhas ao SISTEMA.
    3. Os UTILIZADORES são fieis depositários das suas palavras-passe:
       1. Devem memorizar as palavras-chave dos computadores (i.e. devem ser decoradas);
       2. Não podem divulgar ou escrever as palavras-chave (e.g. papel, etc.), nem fotografar mesmo que seja com o telemóvel pessoal;
       3. Não podem solicitar palavras-passe ou credenciais de outros utilizadores internos ou externos ao SISTEMA;
       4. Devem promover que as palavras-chave sejam inseridas sob total reserva com o objetivo de evitar que estranhos fiquem com acesso irregular ao SISTEMA;
       5. As palavras-chave nunca devem ser guardadas (e.g. *browsers*, sistemas operativos) com o objetivo de não facilitar o acesso por estranhos no caso de invasão do dispositivo (e.g. palavras-chave guardadas no *browser* para acesso facilitado ao e-mail ou às contas bancárias, ficheiros do *word* ou *excel* com as palavras-chave habituais, etc.);
       6. Devem alertar o ADMINISTRADOR DO SISTEMA e o RESPONSÁVEL PELO TRATAMENTO, quando suspeitarem que alguma palavra-chave (sua ou de outro UTILIZADOR) foi comprometida;
       7. Devem solicitar a desativação da sua conta de UTILIZADOR antes da saída da ORGANIZAÇÃO (e.g. cessação de contrato).
    4. O RESPONSÁVEL PELO TRATAMENTO deve:
       1. Notificar o ADMINISTRADOR DE SISTEMA da saída dos UTILIZADORES do SISTEMA para que seja feita a respetiva reconfiguração de acessos e palavras-chave no momento da saída.
    5. O AUDITOR deve:
       1. Avaliar periodicamente que apenas existam contas e perfis de utilizador correspondentes a UTILIZADORES ativos na ORGANIZAÇÃO.
  1. Permissões

As permissões são importantes porque autorizam o acesso aos dados do SISTEMA. A correta criação de perfis e atribuição de permissões garante que apenas os UTILIZADORES autorizados podem consultar ou editar informação, seguindo a estratégia de configuração de recursos definida pelo RESPONSÁVEL PELO TRATAMENTO.

* + 1. O RESPONSÁVEL PELO TRATAMENTO deve:
       1. Definir os perfis de UTILIZADOR nas aplicações operacionais e informar o ADMINISTRADOR DE SISTEMA acerca de quais as permissões de cada um, respeitando o princípio da minimização de privilégios.
    2. O ADMINISTRADOR DE SISTEMA deve:
       1. Configurar os perfis de UTILIZADOR indicados pelo RESPONSÁVEL PELO TRATAMENTO, promovendo que seja obedecido o princípio do mínimo de privilégios para a execução das funções de cada UTILIZADOR na ORGANIZAÇÃO;
       2. Validar periodicamente o respeito pelo princípio da minimização de privilégios em cada perfil.
    3. OS UTILIZADORES devem:
       1. Promover que apenas tenham as permissões suficientes ao exercício das suas funções na ORGANIZAÇÃO, informando o ADMINISTRADOR DE SISTEMA quando o princípio da minimização de privilégios não pareça estar a ser respeitado.
    4. Nos computadores devem ter configuradas:
       1. Uma conta de administrador com permissões de manutenção de sistema operativo sem restrições (incluindo acesso sem restrições às aplicações de segurança);
       2. Uma ou mais contas de utilizador com permissões limitadas que permita apenas acesso aos recursos e aplicações necessárias para que o UTILIZADOR cumpra o seu papel na ORGANIZAÇÃO. Não deve permitir o acesso: i) às configurações do dispositivo; ii) às configurações das aplicações de segurança; e iii) nem devem permitir a instalação ou desinstalação de outras aplicações ou *hardware*.
    5. O acesso aos recursos deve ser sempre controlado através de palavras-chave para garantir o acesso à informação apenas pelos UTILIZADORES autorizados pelo RESPONSÁVEL PELO TRATAMENTO.
    6. Os perfis das aplicações de cariz operacional devem estar devidamente documentados, com o objetivo de garantir apenas acesso estrito à informação necessária ao cumprimento da função de cada UTILIZADOR.
  1. Acessos externos

Os acessos externos constituem um desafio de segurança para o SISTEMA, nomeadamente, porque envolve dispositivos que podem sair da esfera de controlo do ADMINISTRADOR DO SISTEMA e do AUDITOR.

Consideram-se existir acessos externos de dois tipos: i) os eventuais apenas autorizados para fins de suporte técnico; e ii) os acessos permanentes que podem implicar reconfigurações de infraestrutura para disponibilizar o acesso constante.

* + 1. Os acessos externos eventuais para fins de suporte técnico:
       1. Devem ser sempre autorizados pelo RESPONSÁVEL PELO TRATAMENTO;
       2. Apenas é permitido se for utilizada uma ferramenta que implique a validação de acesso através de uma ação explicita de autorização por parte do UTILIZADOR do SISTEMA, e que o conteúdo visto a cada momento entre técnico e UTILIZADOR é o mesmo;
       3. Durante o suporte técnico o UTILIZADOR fica responsável por: i) supervisionar o trabalho efetuado controlando os dados que são vistos e o que é feito com os dados intervencionados; ii) inserir as palavras-chave que forem sido pedidas, avaliando a necessidade de acesso a cada informação e nunca as divulgando; e iii) registar a intervenção técnica indicando o que foi feito e outros dados que considere relevantes de registo.
    2. Os acessos externos permanentes não são admitidos.
    3. Os acessos externos permanentes são admitidos, mas devem:
       1. Estar explicitamente autorizados e justificados pelo RESPONSÁVEL PELO TRATAMENTO identificando que dispositivos e UTILIZADORES ficam autorizados ao acesso externo;
       2. Ser objeto de mitigação de risco pelo ADMINISTRADOR DE SISTEMA, que deve propor e implementar mecanismos de tecnologia de comunicação segura, e de minimização de acesso irregular e de legibilidade de conteúdo transmitido (e.g. utilização de tuneis encriptados, autenticação com vários fatores, ligação apenas autorizada a partir de computadores pertencentes à esfera de administração e auditoria da ORGANIZAÇÃO, etc.);
       3. Ser reavaliados a cada 6 meses de forma a prevenir a acessos autorizados já não necessários, porque representam vulnerabilidades desnecessárias para o SISTEMA.
  1. Dispositivos externos de armazenamento

O SISTEMA deve, por defeito, impedir a utilização de todos os dispositivos externos de armazenamento. Esta medida visa: i) impedir a propagação de *malware* vindo de outros sistemas que pode tornar vulnerável e até dar acesso irregular de estranhos ao SISTEMA; e ii) a cópia não autorizada de dados do SISTEMA.

* + 1. Os dispositivos de armazenamento externo não são admitidos.
    2. Os dispositivos de armazenamento externo são admitidos mas:
       1. Devem ser identificados individualmente;
       2. Devem ser explicitamente autorizados e justificados pelo RESPONSÁVEL PELO TRATAMENTO, identificando que computadores e UTILIZADORES autorizados a utilizar, que informação podem conter, e quais são os locais autorizados onde podem ser encontrados;
       3. A utilização deve ser controlada por aplicações de admissão que garantam a utilização apenas dos DEA configurados como permitidos de utilizar no SISTEMA, e esta aplicação apenas pode ser personalizada ou configurada pelo ADMINISTRADOR DO SISTEMA;
       4. O conteúdo de cada dispositivo de armazenamento externo deve ser ilegível porque podem ser objeto de extravio ou furto. A aplicação de encriptação deverá ser fidedigna (e.g. Deslock da ESET é um produto certificado, BitLocker da Microsoft, etc.);
       5. A necessidade de utilização de dispositivos externos de armazenamento deve ser revisto a cada 12 meses.
       6. No caso de furto ou extravio, o UTILIZADOR autorizado deve proceder à comunicação imediata ao RESPONSÁVEL PELO TRATAMENTO.
  1. Outros dispositivos

Os ataques ao SISTEMA podem ter origem em dispositivos vulneráveis onde é impossível instalar proteções contra *malware* (e.g. router, NAS ou impressora com *firmware* desatualizada).

* + 1. Com o objetivo de proteger estes dispositivos de ataques, o ADMINISTRADOR DE SISTEMA deve:
       1. Promover que a *firmware* dos diferentes equipamentos sejam mantidas atualizadas com as últimas versões estáveis apesar do risco de atualização que significam (o equipamento pode ficar danificado na tentativa de atualização);
       2. Recomendar ao RESPONSÁVEL PELO TRATAMENTO medidas adicionais de segurança de infraestrutura que possam adicionar segurança de forma efetiva e holística ao SISTEMA (*appliances* de segurança).
    2. O RESPONSÁVEL PELO TRATAMENTO deve avaliar em conjunto com o ADMINISTRADOR DE SISTEMA quais as medidas adicionais que podem estar ao alcance do investimento da ORGANIZAÇÃO para mitigar o risco de ataques a partir destes dispositivos.

1. DISPONIBILIDADE E INTEGRIDADE

A disponibilidade e integridade dos dados e do SISTEMA são fatores importantes para garantir o cumprimento das disposições legais em vigor, e para a produtividade e normal funcionamento da ORGANIZAÇÃO.

Neste contexto, o RESPONSÁVEL PELO TRATAMENTO reconhece a importância de dotar o SISTEMA com os mecanismos de disponibilidade e integridade adequados propostos pelo AUDITOR e ADMINISTRADOR DO SISTEMA, pesando sempre com bom senso o esforço de investimento de cada medida proposta e o impacto que pode representar no SISTEMA.

Os UTILIZADORES comprometem-se a utilizar de forma responsável todos os dispositivos e a exercer com zelo o papel de registo que lhes possa ser atribuído. Comprometem-se também a alertar o RESPONSÁVEL PELO TRATAMENTO e o ADMINISTRADOR DE SISTEMA sempre que existam indícios de mau funcionamento de um dispositivo.

* 1. Redundância, resiliência e disponibilidade

A operabilidade do SISTEMA é vital para o funcionamento e sucesso da ORGANIZAÇÃO. Neste contexto o RESPONSÁVEL PELO TRATAMENTO pondera sempre as sugestões feitas pelo AUDITOR e RESPONSÁVEL PELO TRATAMENTO, com o objetivo de promover as propriedades de redundância, resiliência e disponibilidade do SISTEMA.

* + 1. O RESPONSÁVEL PELO TRATAMENTO diz-se preocupado com a disponibilidade do SISTEMA e incita o AUDITOR e o ADMINISTRADOR DE SISTEMA que lhe proponham medidas que promovam a resiliência do SISTEMA, atendendo sempre ao princípio da proporcionalidade entre benefício e investimento, considerando as repercussões negativas da indisponibilidade do SISTEMA e dos dados.
    2. O AUDITOR e ADMINISTRADOR DE SISTEMA devem propor medidas de redundância e disponibilidade ajustadas à realidade da ORGANIZAÇÃO e do SISTEMA para garantir;
       1. A integridade dos dados;
       2. A disponibilidade dos dados;
       3. O mínimo de tempo de paragem do SISTEMA.
  1. Cópias de segurança

As cópias de segurança funcionam como um mecanismo de recurso para recuperar informação perdida. Independentemente da quantidade e qualidade das medidas assumidas pelo RESPONSÁVEL PELO TRATAMENTO para prevenir perda de informação ou inoperabilidade do SISTEMA, existe sempre o risco de perda de informação por avaria, roubo, incêndio, ataque informático, etc. As cópias de segurança são o último recurso na recuperação de dados.

* + 1. O SISTEMA deve contemplar 1 cópia de segurança *online* e 2 *offline*. As cópias *offline* devem ser mantidas fora do contexto físico da ORGANIZAÇÃO obedecendo às regras previstas no Artigo N.º 14 - Dispositivos externos de armazenamento.
    2. As cópias de segurança devem:
       1. Considerar todos os ficheiros e bases de dados do SISTEMA (i.e. todos os dados operacionais devem ser copiados para o dispositivo destino das cópias de segurança);
       2. A execução das tarefas deve ser semiautomática para que o UTILIZADOR tenha a perceção de erros quando e se ocorrerem;
       3. Os dispositivos de armazenamento externo devem apenas ser ligados ao SISTEMA para efetuar a cópia de segurança e devem manter-se ligados apenas durante o tempo de execução da tarefa de cópia;
       4. A reposição deve ser feita pelo ADMINISTRADOR DO SISTEMA sob orientação do RESPONSÁVEL PELO TRATAMENTO;
       5. Em nenhuma circunstância a cópia pode ser deixada sem guarda ou ser disponibilizada a estranhos ao SISTEMA;
       6. A cada 12 meses o ADMINISTRADOR DE SISTEMA deve limpar o destino de cópias de segurança com o objetivo de garantir que apenas existem cópias dos dados que efetivamente são atuais. Esta limpeza deve também ser solicitada ao ADMINISTRADOR DE SISTEMA, sempre que um TITULAR DOS DADOS exerça o seu direito de apagamento de DADOS PESSOAIS.
    3. A disponibilização de cópia de dados para intervenções técnicas externas:
       1. Deve ser autorizada previamente pelo RESPONSÁVEL PELO TRATAMENTO;
       2. Apenas podem ser disponibilizados os dados estritamente necessários à execução daquela tarefa de intervenção técnica;
       3. Antes da disponibilização devem ser avaliados e mitigados os riscos e, no caso de ficheiros indivisíveis (e.g. bases de dados), os dados desnecessários à intervenção técnica em causa devem ser anonimizados.
    4. O RESPONSÁVEL PELO TRATAMENTO deve definir as tarefas de cópias de segurança em conjunto com o ADMINISTRADOR DE SISTEMA identificando:
       1. Os dados a salvaguardar (e.g. ficheiros, bases de dados, etc.);
       2. Os UTILIZADORES responsáveis pela execução das tarefas e verificação de execução das cópias de segurança;
       3. Os UTILIZADORES responsáveis pela execução das tarefas, verificação de execução e validação de conteúdo das cópias de segurança;
       4. A periodicidade em que devem ser executadas;
       5. O tipo de verificação de execução a efetuar (e.g. abertura de um ficheiro na cópia para validação da atualidade do conteúdo, atualidade da data da última alteração do ficheiro, etc.);
    5. Identificar e autorizar os UTILIZADORES que tem a responsabilidade de guardar cópias de segurança fora do contexto físico da ORGANIZAÇÃO, respeitando o Artigo N.º 14 - Dispositivos externos de armazenamento.
    6. O AUDITOR é responsável:
       1. Pela criação e disponibilização aos UTILIZADORES dos instrumentos para registo de execução de cópias de segurança;
       2. Verificar periodicamente os registos preenchidos pelos UTILIZADORES com o objetivo de validar se as tarefas de cópias de segurança e registos de verificação estão a ser executados de forma correta;
       3. Arquivar os registos preenchidos mantendo-os organizados e prontos a serem consultados pelo RESPONSÁVEL PELO TRATAMENTO ou no contexto de alguma auditoria.
  1. Parcerias, contratos e renovações

As parcerias são fundamentais para o funcionamento contínuo do SISTEMA. Manter as parcerias em níveis protocolados é essencial para garantir a operabilidade e o sucesso da ORGANIZAÇÃO.

* + 1. O AUDITOR deve lembrar com antecedência as renovações de contratos e subscrições com o objetivo de evitar:
       1. Paragens do SISTEMA e prejuízos para a ORGANIZAÇÃO;
       2. Tomadas de decisão extemporâneas, i.e. sem margem temporal para avaliar alternativas à renovação.
    2. Neste contexto, o RESPONSÁVEL PELO TRATAMENTO deve:
       1. Promover que as subscrições das aplicações de segurança sejam mantidas sempre ativas com o objetivo de garantir a proteção ininterrupta do SISTEMA;
       2. Promover que todos os dispositivos e aplicações do SISTEMA sejam mantidos ao abrigo de um contrato ou protocolo, formal ou informal, que facilite sem delongas o acesso dos UTILIZADORES a suporte técnico;
       3. Avaliar em conjunto com o ADMINISTRADOR DO SISTEMA e AUDITOR atempadamente as necessidades de renovação de subscrições e contratos.
  1. Revisões periódicas

Existem dispositivos que necessitam periodicamente de substituição de componentes (e.g. consumíveis) ou revisão técnica (e.g. limpeza, lubrificação, etc.) com o objetivo de promover o tempo de vida e bom funcionamento.

* + 1. Assim, incumbe ao RESPONSÁVEL PELO TRATAMENTO:
       1. Promover que todos os dispositivos sejam sujeitos às revisões periódicas se aplicável;
       2. Garantir que cada dispositivo sujeito a revisões periódicas se encontram ao abrigo de um contrato ou protocolo, formal ou informal, que facilite o acesso ao suporte técnico.
    2. O AUDITOR fica com a responsabilidade de lembrar com antecedência as revisões periódicas de dispositivos do SISTEMA com o objetivo de evitar: i) paragens imprevistas e consequentes prejuízos para a ORGANIZAÇÃO; e ii) avarias decorrentes da não revisão atempada dos dispositivos. Além disso, e em conjunto com o ADMINISTRADOR DO SISTEMA, deve promover que:
       1. No máximo a cada 4 anos sejam substituídos os componentes dos computadores considerados como consumíveis ou de desgaste rápido (e.g. pilhas da BIOS, mecanismos mecânicos de refrigeração interna, etc.);
       2. No máximo a cada 3 anos sejam substituídas as baterias e dos dispositivos de equipamentos de redundância elétrica.
  1. Registos

A existência de registos escritos (e.g. de verificação) para monitorizar o SISTEMA, permite aferir acerca da continuidade das verificações feitas pelos UTILIZADORES no tempo.

* + 1. Neste contexto o RESPONSÁVEL PELO TRATAMENTO designa que sejam efetuados os seguintes registos:
       1. A cada 8 dias a verificação de bom funcionamento de equipamentos de redundância elétrica;
       2. A cada 8 dias a verificação de execução de cópias de segurança;
       3. A cada 3 meses a validação de conteúdo de cópias de segurança;
       4. A cada 8 dias a verificação de bom funcionamento de redundância de discos rígidos;
       5. A cada intervenção técnica documentar o que foi feito e quem foi o técnico executor.
    2. Além de designar os registos a serem efetuados pela ORGANIZAÇÃO, o RESPONSÁVEL PELO TRATAMENTO também:
       1. Atribui as responsabilidades de registo a cada UTILIZADOR;
       2. Rever a cada 12 meses essas responsabilidades com o objetivo de manter o tema atual e demonstrar aos UTILIZADORES a importância da integridade dos dados.
    3. Além dos registos já mencionados, o ADMINISTRADOR DO SISTEMA deve:
       1. Manter registo dos incidentes de violação de DADOS PESSOAIS que lhe forem reportados relacionados com o SISTEMA;
       2. Alertar o RESPONSÁVEL PELO TRATAMENTO para a violação ocorrida e aconselhar a notificação das autoridades competentes.

1. OUTRAS REGRAS E BOAS PRÁTICAS

OS UTILIZADORES reconhecem que o SISTEMA é um ecossistema constituído por *hardware*, *software* e utilizadores. Neste contexto, comprometem-se a cumprir com bom senso as regras e procedimentos definidos, tendo sempre por base o objetivo de garantir a privacidade, segurança, integridade e disponibilidade dos dados e do SISTEMA.

Comprometem-se também a comunicar ao RESPONSÁVEL PELO TRATAMENTO, AUDITOR, ou ADMINISTRADOR DE SISTEMA, qualquer anomalia ou suspeição de anomalia que ocorra no SISTEMA, assumindo sempre que a cautela redobrada é preferível à imprudência exagerada.

* 1. Internet

A internet é a origem de muitos riscos e problemas para os sistemas. Apesar das vantagens que oferece, são muitas as ameaças e vulnerabilidades exploradas a partir da internet.

O e-mail é uma das ferramentas mais utilizadas pela ORGANIZAÇÃO. No entanto, é também o ponto de entrada de muitas ameaças para os sistemas.

* + 1. Neste contexto, o RESPONSÁVEL PELO TRATAMENTO:
       1. Proíbe a utilização de e-mails não oficiais da ORGANIZAÇÃO (e.g. emails particulares);
       2. Proíbe a utilização de e-mails da ORGANIZAÇÃO para fins que não os relacionados com o exercício das funções operacionais de cada UTILIZADOR. i.e., os UTILIZADORES estão proibidos de utilizar o e-mail da ORGANIZAÇÃO para fins pessoais;
       3. Promove a utilização de endereços de e-mail anónimos com o objetivo de evitar a identificação direta ou indireta de TITULARES DOS DADOS;
       4. Deve avaliar caso a caso a necessidade de disponibilizar os serviços de internet a cada equipamento e a cada UTILIZADOR (e.g. navegação, e-mail, etc.).
    2. O ADMINISTRADOR DE SISTEMA deve:
       1. Prevenir a legibilidade de conteúdo de e-mail durante a transmissão na internet;
       2. Avaliar os custos e propor ao RESPONSÁVEL PELO TRATAMENTO a utilização de certificados digitais para assinar digitalmente e-mails;
       3. Avaliar a possibilidade de configuração das contas de e-mail utilizando mecanismos de redundância de informação no servidor (e.g. IMAP), ou considerar os repositórios de e-mail nas tarefas de cópias de segurança.
    3. O AUDITOR, em conjunto com o ADMINISTRADOR DE SISTEMA, devem estudar medidas de mitigação de risco na utilização da internet, propondo:
       1. A utilização de listas de *sites* proibidos ou permitidos;
       2. Mecanismos de controlo de navegação, *downloads* e de *Instant Messaging* (IM) (e.g. Facebook, WhatsApp, Skype, etc.);
       3. A definição de regras para restringir o envio ou receção de e-mails com base numa lista fechada de endereços de contacto.
    4. Os UTILIZADORES devem:
       1. Utilizar a internet conscientes dos riscos, evitando aceder ou fazer *downloads* de sites de origem não fidedigna;
       2. Avaliar cuidadosamente os e-mails recebidos antes de os abrir. A análise prévia da origem, pertinência e atualidade de conteúdo, podem evitar ataques ao SISTEMA. Em caso de dúvida, o UTILIZADOR deve confirmar o envio, por outra via, com o remetente;
       3. Manter nos recipientes (i.e. caixa a receber, enviados, etc.) apenas os e-mails com sentido e pertinência para a ORGANIZAÇÃO, i.e. eliminando de forma definitiva os e-mails que não sejam de interesse para a ORGANIZAÇÃO.
  1. Hardware e software

A estabilidade do SISTEMA está intrinsecamente relacionada com a forma como os UTILIZADORES usam e respeitam os equipamentos e aplicações. Cuidar do *hardware* e respeitar o *software* são pressupostos importantes para o bom funcionamento do SISTEMA.

* + 1. Neste contexto, o UTILIZADOR compromete-se a:
       1. Utilizar com bom senso todos os equipamentos e aplicações do SISTEMA;
       2. Não instalar ou desinstalar aplicações sem a supervisão do ADMINISTRADOR DO SISTEMA;
       3. Não fornecer acesso ao SISTEMA, presencial ou remotamente, sem autorização clara do RESPONSÁVEL PELO TRATAMENTO;
       4. Nunca divulgar detalhes técnicos, nem credenciais de acesso, mesmo que se trate da troca ou instalação de um dispositivo, a não ser com autorização do RESPONSÁVEL PELO TRATAMENTO ou ADMINISTRADOR DO SISTEMA;
       5. Não deixar que os equipamentos ou aplicações sejam manuseadas por pessoal não autorizado, mesmo que essas pessoas detenham as competências apropriadas para o efeito;
       6. Nunca fazer partilha de dados, seja através de recursos de rede internos ou externos, ou através de dispositivos externos de armazenamento, a não ser quando autorizados e previstos pelo RESPONSÁVEL PELO TRATAMENTO.
    2. O RESPONSÁVEL PELO TRATAMENTO compromete-se a:
       1. Avaliar cuidadosamente todos os pedidos de acesso presenciais ou remotos ao SISTEMA;
       2. Promover a privacidade total do SISTEMA, não autorizando intervenções técnicas em dispositivos ou aplicações sem a presença do ADMINISTRADOR DO SISTEMA;
       3. Não permitir a saída de equipamentos ou aplicações para intervenções técnicas externas, sem avaliar com o ADMINISTRADOR DO SISTEMA a real necessidade da saída e a utilização de medidas de contenção de risco (e.g. retirar disco rígido com informação).
    3. O ADMINISTRADOR DE SISTEMA fica com a responsabilidade de:
       1. Promover que todas as aplicações, *browsers* e componentes (e.g. *flash player*, *java*, etc.) estejam devidamente atualizadas, ponderando sempre com antecedência a compatibilidade da atualização com o SISTEMA e o risco de proceder à atualização.
  1. Informação

O SISTEMA guarda e processa dados que constituem informação e conhecimento, que são utilizados na operacionalização da atividade da ORGANIZAÇÃO e como suporte à tomada de decisões pelo RESPONSÁVEL PELO TRATAMENTO.

* + 1. Assim, RESPONSÁVEL PELO TRATAMENTO deve:
       1. Promover que a informação do SISTEMA se mantenha organizada e atualizada;
       2. Promover que o SISTEMA apenas contenha os ficheiros e bases de dados necessárias à operação da ORGANIZAÇÃO, com o objetivo de facilitar a localização dos dados e o cumprimento atempado das obrigações previstas na lei;
       3. Implementar políticas de apagamento consciente da informação em desuso;
       4. Rever periodicamente que apenas exista informação atual e necessária no SISTEMA;
       5. Aquando da saída da ORGANIZAÇÃO de um UTILIZADOR, promover que os dispositivos por ele utilizados sejam entregues a outro UTILIZADOR sem qualquer tipo de informação pessoal (ambos UTILIZADORES devem assinar um documento a confirmar a passagem dos dispositivos sem informação pessoal).
    2. Os UTILIZADORES devem:
       1. Seguir as regras definidas pelo RESPONSÁVEL PELO TRATAMENTO para manter a informação organizada e atualizada;
       2. Guardar apenas a informação de suporte à operacionalidade e tomada de decisões da ORGANIZAÇÃO;
       3. Nunca utilizar os dispositivos da ORGANIZAÇÃO para fins pessoais;
       4. Não tratar informação além da que é de interesse funcional para a ORGANIZAÇÃO;
       5. Aquando da saída da ORGANIZAÇÃO (e.g. cessação de contrato, despedimento, etc.), apagar de forma definitiva toda a informação pessoal, mantendo apenas aquela que seja pertinente para a atividade da ORGANIZAÇÃO.
    3. O AUDITOR deve:
       1. Verificar com regularidade a existência de ficheiros e bases de dados não alterados nos últimos 12 meses;
       2. Verificar regularmente a existência de ficheiros ou bases de dados em duplicado ou desnecessárias no SISTEMA (e.g. clones de base de dados para testes).
    4. O ADMINISTRADOR DE SISTEMA deve:

Aquando da saída de um UTILIZADOR da ORGANIZAÇÃO, avaliar a possibilidade de existirem DADOS PESSOAIS (e.g. no e-mail, em ficheiros, etc.), com o objetivo de evitar incidentes de violação de DADOS PESSOAIS por outros UTILIZADORES, e aconselhar o RESPONSÁVEL PELO TRATAMENTO acerca de medidas de reação para aquele caso em concreto e para prevenir outros no futuro.

* 1. Formação

Um SISTEMA é um ecossistema formado por vários tipos de componentes sendo um deles os UTILIZADORES. Enquanto humanos as pessoas nem sempre ajuízam corretamente as suas ações. A formação pode ajudar os UTILIZADORES a melhor entenderem e desempenharem o seu papel no SISTEMA.

O RESPONSÁVEL PELO TRATAMENTO acredita que, se prestada periódica e regularmente, a formação pode contribuir para manter atual o tema da segurança e da privacidade. Pode também contribuir para a diminuição dos níveis de: i) erraticidade dos UTILIZADORES; ii) violação do regulamento de SISTEMA; e iii) violação de legislação em vigor (e.g. violação de DADOS PESSOAIS). A formação pode também ajudar os UTILIZADORES na identificação de violações de DADOS PESSOAIS.

* + 1. O AUDITOR em conjunto com o RESPONSÁVEL PELO TRATAMENTO devem avaliar as necessidades de formação conjunta ou individual por UTILIZADOR, com o objetivo de:
       1. Promover uma mudança do *mindset* em função dos princípios defendidos pelo RGPD;
       2. Formar os UTILIZADORES para que saibam identificar ocorrências de violação de DADOS PESSOAIS e percebam a importância de os comunicar ao RESPONSÁVEL PELO TRATAMENTO para tratamento e registo;
       3. Dotar os UTILIZADORES com os conhecimentos necessários para que saibam evitar ataques (e.g. *phishing*);
       4. Promover a rotina da dupla verificação de destinatários e conteúdo no envio de mensagens (e.g. email, Facebook, WhatsApp, etc.);
       5. Promover os processos de anonimização e mobilidade segura de dados (i.e. ilegíveis por estranhos);
       6. Promover a política de minimização de dados tratados e ficheiros presentes no SISTEMA;
       7. Alterar a forma de pensar acerca do tratamento e partilha de dados;
       8. Promover a proteção no acesso aos equipamentos e aplicações;
       9. Promover que apenas sejam colocados dados nos recursos previstos pelo RESPONSÁVEL PELO TRATAMENTO e nunca localmente nos computadores;
       10. Promover a existência no SISTEMA de, apenas, os ficheiros necessários à operabilidade da ORGANIZAÇÃO;
       11. Enfatizar a importância de manter cópias de segurança atualizadas, desligadas do SISTEMA e guardadas em localizações externas ao domínio físico da ORGANIZAÇÃO;
       12. Promover o cumprimento e sugerir alterações ao RESPONSÁVEL PELO TRATAMENTO para melhoria deste regulamento;
       13. Promover políticas de verificação e atualização de aplicações de *malware* e do sistema operativo (e.g. reinícios de sistema operativo ao final do dia).

1. AUDITORIAS

O RESPONSÁVEL PELO TRATAMENTO considera que a segurança, privacidade, integridade e disponibilidade dos dados são temas que tem que ser revistos periodicamente, por causa do dinamismo e da evolução dos componentes que constituem o SISTEMA.

O aumento de funcionalidades e modernização das aplicações são sempre recebidas com apreço pelos UTILIZADORES. No entanto, acarretam também novas vulnerabilidades e necessidades de correção. As atualizações de segurança são mecanismos de reação utilizadas pelos fabricantes para mitigar ou extinguir os riscos entretanto detetados nas suas aplicações. Uma das funções do AUDITOR é validar que essas correções são implementadas nos sistemas.

* 1. Objetivo

As auditorias visam contribuir para que o SISTEMA mantenha bons níveis de segurança, privacidade, integridade e disponibilidade dos dados.

* + 1. Neste contexto, o RESPONSÁVEL PELO TRATAMENTO assume como necessário delegar a responsabilidade de auditoria ao AUDITOR para que:
       1. Promova o cumprimento deste regulamento;
       2. Promova a privacidade, segurança, disponibilidade e integridade dos dados;
       3. Promova o bom funcionamento do SISTEMA com o objetivo de evitar interrupções não previstas.
    2. O AUDITOR deve:
       1. Organizar a informação relacionada com o SISTEMA e com as auditorias;
       2. Manter o responsável informado acerca de vulnerabilidades encontradas e propor medidas corretivas;
       3. Propor recomendações ao RESPONSÁVEL PELO TRATAMENTO que visem promover a segurança, privacidade, integridade e disponibilidade dos dados;
       4. Exercer com zelo todas as suas tarefas de auditoria.

1. CONCLUSÃO

Este documento demonstra o compromisso da ORGANIZAÇÃO em cumprir a legislação que regula as questões de privacidade, segurança, integridade e disponibilidade do SISTEMA. Através dele, o RESPONSÁVEL PELO TRATAMENTO pretende implementar regras e procedimentos que sejam conducentes à conformidade com a legislação em vigor (e.g. RGPD).

O RESPONSÁVEL PELO TRATAMENTO deve promover revisões deste documento sempre que necessário, com o objetivo de o melhorar iterativamente, mas também para acompanhar a evolução tecnológica e o aparecimento de novos desafios de segurança.

RESPONSÁVEL PELO TRATAMENTO e UTILIZADORES assinam todas as novas versões deste documento. Um novo UTILIZADOR deve também assinar aquando do seu acolhimento na ORGANIZAÇÃO.

Este regulamento entra em vigor a «*2000-01-01*».

O RESPONSÁVEL PELO TRATAMENTO determina que este regulamento seja cumprido,

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
«*Nome completo do RESPONSÁVEL PELO TRATAMENTO*»

OS UTILIZADORES declaram terem lido o regulamento e não existirem dúvidas que impeçam o seu cumprimento,

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_